## REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-23 are pending in the application, with Claims 1-7, 9-16 and 18-22 amended and Claim 23 added by the present amendment.

In the Official Action, Claims 1-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Caronni (U.S. Patent No. 6,507,908) in view of Inoue et al. (U.S. Patent No. 6,170,057, hereinafter Inoue).

Claims 1-7, 9-16 and 18-22 are amended to clarify features therein. Support for these amendments is found in Applicants' originally filed specification. No new matter is added.

Briefly recapitulating, Claim 1 is directed to a gateway device for carrying out a packet relaying at a transport or upper layer between a sender device and a destination device which are capable of carrying out communications through networks with data secrecy based on a security association set up therebetween. The gateway device includes a security information management unit configured to obtain and manage information regarding ~~a~~ the security association; a data receiving unit configured to receive data first packet which includes a first header and an encrypted packet from the sender device; and a data decryption unit configured to decrypt the encrypted packet to obtain a second packet including a second header and data by utilizing the information regarding the security association and to check the second header. The device also includes a packet relay unit configured to carry out the packet relaying at the transport or upper layer according to the second header; a data encryption unit configured to encrypt the second packet to obtain an encrypted second packet by utilizing the information regarding the security association, no header being newly attached to the encrypted second packet; and a data transmitting unit configured to transmit the encrypted second packet with attaching the first header to the destination device.

As described in Applicants' specification, one object of the present invention is to effectively combine a method for providing security such as IPSec and a device, such as a TCP-GW, and a Snoop proxy particularly provided between wired side terminal devices and wireless side terminal devices, for improving performance of TCP. Thus, the gateway is located between a first terminal device and a second terminal device. The first and second terminal devices are in security association with each other and thus carry out communications with each other with data secrecy based on the security association. The gateway obtains information regarding the security association from somewhere. This is because the gateway itself does not have a function to secure secret communications between the first device and the second device. The gateway is provided as a proxy device for improving performance of TCP.

A gateway device according to the present invention carries out a packet relaying at a transport or upper layer between a sender device and a destination device which are capable of carrying out communications through networks with data secrecy based on a security association set up therebetween. A security information management unit in the gateway device obtains and manages information regarding the security association. A data receiving unit receives a first packet which includes a first header and an encrypted packet from the sender device, and then a data decryption unit decrypts the encrypted packet to obtain a second packet including a second header and data by utilizing the information regarding the security association and checks the second header. Then, a packet relay unit carries out the packet relaying at the transport or upper layer according to the second header. On the other hand, a data encryption unit encrypts the second packet to obtain an encrypted second packet by utilizing the information regarding the security association, no header being newly attached to the encrypted second packet; and then a data transmitting unit transmits the encrypted second packet with attaching the first header to the destination device.

Caronni describes a method for secure data communications with a mobile machine in which a data packet is received from the mobile machine having a particular network address. A pool of secure addresses is established and a data structure is created to hold address translation associations. Each association is between a particular network address and a particular one of the secure addresses. If the received data packet is a secure data packet an association between the received data packets network address and a secure address in the data structure is identified and the data packets network address is translated to the associated secure address before forwarding the data packet onto higher network protocol layers. When the received data packet is not secure it is passed on without address translation to the higher network protocol layers. For outgoing packets addressed to a secure address, the secure address is translated to a real network address and the packet payload is encrypted. Outgoing packets that are addressed directly to the real network addresses are passed through in a conventional manner.[1] However, as acknowledged in the Official Action, while Caronni decrypts data from an external device, Caronni does not decrypt the data according to the information regarding the security association.

Inoue describes a mobile computer and a packet encryption and an authentication method which are capable of controlling an activation of a packet encryption and authentication device belonging to the mobile computer according to the security policy at the visited network of the mobile computer. The mobile computer is provided with a packet encryption and authentication unit having an on/off switchable functional for applying an encryption and authentication processing on input/output packets of the mobile computer. One of the packet encryption authentication unit and an external packet processing device is selectively controlled to carry out the encryption and authentication processing on the input/output packets, where the external packet processing device being provided in a visited

[1] Caronni Abstract.

network at which the mobile computer is located and having a function for relaying packets transferred between a computer located in the network and a computer located in another network by applying the encryption and authentication processing.[2]

However, contrary to the Official Action, like Caronni, Inoue fails to disclose or suggest the feature that "a data decryption unit configured to decrypt the encrypted packet to obtain a second packet including a second header and data by utilizing the information regarding the security association and to check the second header; a packet relay unit configured to carry out the packet relaying at the transport or upper layer according to the second header; and a data encryption unit configured to encrypt the second packet to obtain an encrypted second packet by utilizing the information regarding the security association, no header being newly attached to the encrypted second packet". In Applicants' claimed invention, the second header is obtained by decrypting the encrypted packet included in the first packet received by the receiving unit. Then, the packet relay unit carries out the packet relaying at the transport or upper layer according to the obtained second header. The data encryption unit encrypts the second packet to obtain an encrypted second packet, and then the transmitting unit transmits the encrypted second packet with attaching the first header. In this process, no header is newly added the packet. Both Caronni and Inoue fail to disclose or suggest these features.

Column 2, lines 42-49 in Inoue merely describes "gateway 4a (where the packet is decrypted) 6 home agent (HA) 4 6 getaway 4a (where the packet is encrypted again)". Sending and receiving a packet between the decryption and encryption is quite different from decrypting a packet, using the decrypted packet and then re-encrypting the packet. Column 5, lines 30-42 in Inoue describes that "the data routing control with respect to the mobile computer 2 is carried out by encapsulating an IP packet destined to an original address (an

[2] Inoue, Abstract.

address in a home network la) of the mobile computer 2 within a packet destined to a current location address of the mobile computer 2". Furthermore, column 5, lines 43-50 in Inoue merely describes that "each gateway has a packet encryption and authentication processing function". Column 7, lines 55-65 in Inoue discloses that "the gateway 6 applies the encryption and authentication processing to both the packet that is received from the Internet 6 and is sent to the mobile station 2 and the packet that is received from the mobile station 2 and is sent to the Internet 6". Each of these portions of Inoue fail to disclose or suggest the features discussed above.

The Advisory Action states Inoue discloses a gateway system with a data packet relaying function that decrypts the received encrypted data packets and re-encrypts the same data packets before transmitting them to their destination (col. 2, lines 42-49 and col. 5, lines 30-42). However, as apparent from col.2, lines 42-49 in Inoue, such a function is carried out by a plurality of gateways (4c, 4a) and via another device (home agent (HA)). In contrast, one gateway carries out such a function according to the present invention. However, Claims 1, 19 and 21 include the limitation "the gateway does not attach a new destination address to data to be transmitted before encrypting the data" (emphasis added) to clearly point out that one gateway decrypts received data and then encrypts the decrypted data.

Furthermore, Applicants continue to traverse the finding that Caronni describes a security association between first and second devices. That is, in Caronni, only an internal secure network is secured from an external terminal such as a mobile device. The gateway recited in Applicants' claims decrypts encrypted data received from the first terminal device or the second terminal device according to the information regarding the security association. In addition, the gateway recited in Applicants' independent claims relays data at a transport or upper layer according to the decrypted data. Caronni falls to disclose or suggest any data relaying operation, let alone Applicants' recited relay at a transport or upper layer according

to the decrypted data. By relaying at a transport or upper layer according to the decrypted data, the claimed invention is provided as a proxy device for improving performance of TCP, whereas the gateway in Caronni merely maintains access control lists (ACLs) to prevent unauthorized devices from accessing the secure network. Similarly, Caronni does not encrypt the data according to the information regarding the security association. Inoue fails to cure the deficiencies of Caronni.

The gateway recited in Claims 10, 20 and 22 does not have a decryption/encryption function as recited in Claims 1, 19 and 21, but does include an authentication function to attach authentication information to data to be transmitted to the second terminal device or the first terminal device, according to the information regarding the security association. Caronni fails to teach or suggest such an authentication operation.

New Claim 23 is directed to another aspect of the present invention. Claim 23 differs from amended Claim 1 by reciting "receiving the second packet directly from the decryption unit" instead of the limitation "no header being newly attached to the encrypted second packet." That is, the data encryption unit receives the second packet directly from the decryption unit and encrypts the second packet to obtain an encrypted second packet by utilizing the information regarding the security association. Inoue teaches away this feature definitely since the packet decrypted at the gateway 4a is once sent to the Home Agent 5 and then returns to the gateway 4a and then encrypted there in Inoue.

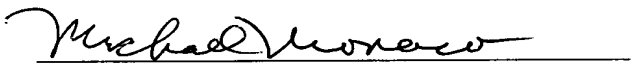
MPEP §706.02(j) notes that to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Also, the teaching or suggestion to

make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Without addressing the first two prongs of the test of obviousness, Applicants submit that the Official Action does not present a *prima facie* case of obviousness because both Caronni and Inoue fail to disclose all the features of Applicants' claimed invention.

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action that that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\atty\Mm\AMENDMENT\208915US-am.doc